UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

CONVERGEN ENERGY LLC, L'ANSE WARDEN ELECTRIC COMPANY, LLC, EUROENERGY BIOGAS LATVIA LIMITED, and LIBRA CAPITAL US, INC.

Plaintiffs,

-against-

STEVEN J. BROOKS, NIANTICVISTA ENERGY LLC, GREGORY MERLE, RIVERVIEW ENERGY CORPORATION, DANIEL ESCANDON GARCIA, RAMON URIARTE INCHAUSTI, CHIPPER INVESTMENT SCR, SA, URINCHA SL, THEODORE JOHN HANSEN, BRIAN R. MIKKELSON, and CONVERGEN ENERGY WI, LLC,

Defendants.

Index No. **1:20-cv-03746** (LJL)

DECLARATION OF AARON S. WEISS

I, Aaron S. Weiss, declare as follows:

1. I am the principal analyst and owner of Forensic Recovery, LLC, and I was engaged by Seiden Law Group, LLP ("**SLG**") to consult and provide forensic analysis regarding digital evidence in this matter.

2. I received both a Bachelor of Science in Computer Science and a Master of Science in Digital Forensics from the University of Central Florida in Orlando, Florida. I have received hundreds of hours of training related to the preservation, collection, and analysis of digital evidence. I have worked as a digital forensic analyst since 2010.

3. I have authored and instructed undergraduate courses on digital investigation and electronic discovery, and I have presented at conferences and meetings on related subjects.

4. I have worked on more than 200 cases related to digital investigations, and I have testified as an expert in both civil and criminal state and federal courts approximately 15 times. Each case typically involves forensically investigating many devices.

Background

5. Between June 19, 2020, and June 21, 2020, I remotely generated a forensic image of an HP notebook computer (Model: Probook 430 G3, System Name: "SBROOKS218-LPT"; Operating System: Windows 10 Pro) (the "**Laptop**"), which was in the possession of Ryan Billings, Esq. ("**Billings**") of Kohner, Mann & Kailas. Billings then mailed me the forensic image, which had been stored on an external hard drive for this purpose.

6. I understand from SLG that the Laptop was provided by Libra Capital US, Inc. ("**Libra**"), to Steven Brooks ("**Brooks**") as an employee for work purposes.

7. SLG asked me to perform the forensic analysis of the Laptop and share my findings. The analysis was focused on identifying USB devices, attempts to delete data or otherwise unusual activity. My ongoing analysis to date has focused on user activity after January 1, 2020.

Summary of Findings

8. There is evidence of activity on the Laptop used by Steven Brooks and returned in June 2020 that is inconsistent with activity that would be expected on a computer used by a finance professional. The software applications identified throughout this declaration are some that I or other information technology security professionals would use.

9. Forensic artifacts identified during my analysis of this Laptop indicate that documents important to this case exist on other devices and accounts, including, but not limited

to, USB devices, other computers, and cloud-based storage accounts used by Brooks. None of the devices or accounts identified in this declaration have been provided for analysis.

10. Ten (10) different USB storage devices were connected to the Laptop on or after February 3, 2020. None of the devices or accounts identified in this declaration have been provided for analysis.

11. A Microsoft OneDrive account associated with stevebrooks17@gmail.com was synchronized to the Laptop. My analysis found files with names indicative of being related to Libra to be in the OneDrive account; however, the contents of the files are not viewable on the Laptop. Preservation and analysis of the OneDrive account would be necessary to view the contents of these files.

12. There is evidence of behavior consistent with an attempt to communicate securely using encrypted email or messages.

13. There is evidence of the mass deletion of files on March 24, 2020 and May 31, 2020, just prior to the return of the computer.

14. On March 16, 2020 and March 23, 2020, repeated failed attempts to logon to the administrator account were made. The administrator account would have had full access to make changes to the system, while the "Steven Brooks" user account did not. Based on the findings below and the totality of the circumstances, this activity suggests the user was attempting to gain access to an administrator account it doe not have the password for.

15. Several forensic artifacts indicate that attempts were made to create a bootable environment that can be launched from a USB device; there is also evidence that a bootable environment was downloaded. A bootable USB environment can be used to copy, modify, or delete data without leaving execution artifacts on the target system.

16. The amount of unusual and type of activity observed leading up to the return of the Laptop caused the irreversible overwriting of previously deleted data.

USB Devices Connected to the Laptop

17. My forensic analysis of the Laptop has revealed that at least 11 distinct USB drives/external hard drives ("**USB Drives**") were connected to the Laptop on or after February 3, 2020. The following details were obtained pertaining to the USB Drives.

Serial Number	Friendly Name	Last Insertion Date/Time - UTC-05:00 (M/d/yyyy)[DST]	Last Removal Date/Time - UTC-05:00 (M/d/yyyy)[DST]	**First Installed Date**
575839314543354645555850 (WX91EC5FEUXP in ASCII)	WD My Passport 25E2 USB Device	5/31/2020 16:21	5/31/2020 16:27	2/28/2020 19:06
14090585000059	USB Device	3/25/2020 20:58	3/25/2020 21:19	3/24/2020 04:28
0700016F37F33844	PNY USB 3.0 FD USB Device	3/24/2020 05:46	3/24/2020 06:16	3/17/2020 00:12
14090585000071	USB Device	3/24/2020 05:45	3/24/2020 5:46	3/24/2020 04:39
14090585000008	USB Device	3/24/2020 05:44	3/24/2020 05:44	3/17/2020 02:13
07751009D111EBDD	SanDisk SanDisk Cruzer USB Device	3/23/2020 15:28	3/23/2020 13:46	3/17/2020 07:26
14090585000045	USB Device	3/23/2020 15:23	3/23/2020 15:23	3/17/2020 07:22
07139AAE9151A212	PNY USB 3.0 FD USB Device	3/17/2020 06:18	3/17/2020 06:18	3/17/2020 02:23
14090500000019	USB Device	3/17/2020 02:37	3/17/2020 03:23	3/17/2020 02:12
00000000000050E2	IT1165 USB Flash Disk USB Device	2/03/2020 11:13	2/05/2020 13:35	9/23/2019 10:51

Data Copied to External Drive

18. A series of folders were placed on a Western Digital My Passport external USB hard drive with Volume Serial Number: FC29D642. The target creation date and time indicates

the folders were placed in the \backup\ folder sequentially on May 31, 2020. I know this from my review of LNK file artifacts found on the Laptop. Windows-created LNK files[1] are generated when a user opens a file, document, or application, and they contain metadata about the target file even after the target file is moved or deleted.

Linked Path	Target File Created Date/Time - UTC-05:00 (M/d/yyyy)[DST]
F:\backup\Union dEI	5/31/2020 16:27
F:\backup\WILTW	5/31/2020 16:27
F:\backup\Project Havana	5/31/2020 16:27
F:\backup\Riposte	5/31/2020 16:27
F:\backup\Spanish Real Estate	5/31/2020 16:27
F:\backup\Principal Media	5/31/2020 16:26
F:\backup\Office and Phone	5/31/2020 16:26
F:\backup\Personal Finance	5/31/2020 16:26
F:\backup\Mint - Montebalito	5/31/2020 16:26
F:\backup\MFG Owners MTG	5/31/2020 16:26
F:\backup\MFG Refi - 2016	5/31/2020 16:26
F:\backup\Mercovil	5/31/2020 16:26
F:\backup\LXM	5/31/2020 16:26
F:\backup\Libra Trave1\7	5/31/2020 16:26
F:\backup\Lomar	5/31/2020 16:26
F:\backup\Libra Research	5/31/2020 16:26
F:\backup\Libra Presenations	5/31/2020 16:26
F:\backup\Libra Group Logo + Letterhead	5/31/2020 16:26
F:\backup\Libra Interns	5/31/2020 16:26
F:\backup\Libra Expenses	5/31/2020 16:26
F:\backup\Internal Review	5/31/2020 16:26
F:\backup\La Dolfina	5/31/2020 16:26
F:\backup\Hotel - Financial Models	5/31/2020 16:26
F:\backup\Hotels - TD Meeting	5/31/2020 16:26
F:\backup\IDB	5/31/2020 16:26
F:\backup\GWF	5/31/2020 16:25
F:\backup\GWE	5/31/2020 16:25
F:\backup\GML	5/31/2020 16:25
F:\backup\Grace Hotels	5/31/2020 16:25
F:\backup\FNA	5/31/2020 16:25
F:\backup\Financial Models	5/31/2020 16:25

[1] https://www.magnetforensics.com/blog/forensic-analysis-of-lnk-files/

Linked Path	Target File Created Date/Time - UTC-05:00 (M/d/yyyy)[DST]
F:\backup\Financial Results	5/31/2020 16:25
F:\backup\FCA Houston	5/31/2020 16:25
F:\backup\FCA Brazil	5/31/2020 16:25
F:\backup\FCA BoD	5/31/2020 16:25
F:\backup\FCA - Brazil Capital Raise	5/31/2020 16:25
F:\backup\FCA	5/31/2020 16:24
F:\backup\Euro Energy	5/31/2020 16:24
F:\backup\Camuzzi Gas	5/31/2020 16:24
F:\backup\CEN+WOL Refi 2016	5/31/2020 16:24
F:\backup\Athens Marathon 2017	5/31/2020 16:24
F:\backup\Ameris II	5/31/2020 16:24
F:\backup\Argentina	5/31/2020 16:24
F:\backup\Windows\OneDriveTemp	5/31/2020 16:01
F:\backup\Windows\SWSETUP	5/31/2020 16:01
F:\backup\Windows\hp	5/31/2020 16:01
F:\backup	5/31/2020 16:00

19. The same folders[2] are located on the Laptop under the "\Users\Steven Brooks\Desktop\Toshiba 2014-2018" folder. This represents at least 4,149 files. While I cannot verify that all those files were on the USB drive, the same folders were placed on it sequentially, so there is good reason to believe they contain the same files. The folders were on the Laptop were also not subsequently modified.

USN Journal Data

20. As part of my forensic review, I reviewed USN Journal Entries. The USN Journal is a persistent log of all changes made to files on a volume; it records file and directory creations, deletions, renames, and moves.

21. Files recorded in the USN Journal as being deleted may not be recoverable for various reasons. For example, a Solid State Hard Drive running Windows 10, such as the

[2] The "Libra Trave1\7" on the external hard drive does not match the name "Libra Travel" on "Toshiba 2014-2018" folder and is not counted among the 4,149 files.

internal hard drive installed in this Laptop, will erase unused blocks on an ongoing basis in order to prevent performance degradation over time. An effect of this function is the increased chance that a deleted file will be unrecoverable once it is deleted and removed from the recycle bin. Space previously allocated to deleted files can be allocated to new files, and thus, making the original file unrecoverable.

22. The following table identifies entries in the USN Journal for files or directories that were deleted since March 24, 2020. The full USN Journal can be provided upon request.

File Name	Timestamp Date/Time - UTC-05:00 (M/d/yyyy)[DST]
downloads3.txt	3/24/2020 04:32:44
guaranty.lnk	3/24/2020 04:36:46
cleanup x.lnk	3/24/2020 04:37:19
L'Anse - DTE PPA.lnk	3/24/2020 04:37:38
cleanup x.lnk	3/24/2020 04:37:38
CEL - Luminor_102019.lnk	3/24/2020 04:37:48
cleanup x.lnk	3/24/2020 04:37:48
CE Latvia Group 2014-Q3 2019 Revenue.lnk	3/24/2020 04:37:53
cleanup x.lnk	3/24/2020 04:37:53
AC Power Download	3/24/2020 04:47:07
utc.app.json.new	5/31/2020 15:54:56
utc.privacy.json.new	5/31/2020 15:54:56
Brighten Video.man.igpi	5/31/2020 15:54:57
Darken Video.man.igpi	5/31/2020 15:54:57
Init[1].htm	5/31/2020 15:55:04
snapshot.etl	5/31/2020 15:57:39
Devices and Printers (3).lnk	5/31/2020 15:58:12
LWEC-Convergen Energy WI Pellet Supply Agreement 30Nov2019 dpc.lnk	5/31/2020 15:58:12
promissory.lnk	5/31/2020 15:58:12
MSHist012020041320200414	5/31/2020 16:00:17
MSHist012020040620200413	5/31/2020 16:00:17
MSHist012020032320200330	5/31/2020 16:00:17
clark kent.lnk	5/31/2020 16:00:17
My Passport (F).lnk	5/31/2020 16:00:17
This PC.lnk	5/31/2020 16:00:17
$IP32FNQ	5/31/2020 16:02:50
Downloaded from Demonoid - www.dnoid.to.txt	5/31/2020 16:02:50

File Name	Timestamp Date/Time - UTC-05:00 (M/d/yyyy)[DST]
Downloaded from HaxNode.CoM.txt	5/31/2020 16:02:50
Freemake Video Converter 4.1.10.393 Final + Serial.zip	5/31/2020 16:02:50
Torrent Downloaded from Glodls.to.txt	5/31/2020 16:02:50
[TGx]Downloaded from torrentgalaxy.to .txt	5/31/2020 16:02:50
$RP32FNQ	5/31/2020 16:02:50
$R3S5S35.JPG	5/31/2020 16:03:02
$I3S5S35.JPG	5/31/2020 16:03:02
$IUNDJLW	5/31/2020 16:03:10
.VideoCleaner_settings.txt	5/31/2020 16:03:10
Adam fund manager cover letter.docx	5/31/2020 16:03:10
350c0eddc1955_results.csv	5/31/2020 16:03:10
address.docx	5/31/2020 16:03:10
all al orders.xlsx	5/31/2020 16:03:10
ALTON LANE NOTES WIFI COMPUTER.PNG	5/31/2020 16:03:10
another meredith letter.docx	5/31/2020 16:03:10
Ansanko Gold Northern Right Final 2.docx	5/31/2020 16:03:10
Ansanko Gold Northern Right Final 3.docx	5/31/2020 16:03:10
Ansanko Gold Northern Right Final 4.docx	5/31/2020 16:03:10
Ansanko Gold Northern Right Final.docx	5/31/2020 16:03:10
Ansanko Gold Northern Right Final.pdf	5/31/2020 16:03:10
Ansanko Gold Northern Right.docx	5/31/2020 16:03:10
Ansanko mining 2.docx	5/31/2020 16:03:10
Ansanko mining.docx	5/31/2020 16:03:10
Asanko Gold - Northern Right.docx	5/31/2020 16:03:10
Asanko Gold - Northern Right.pdf	5/31/2020 16:03:10
atomic bitcoin wallet backup.txt	5/31/2020 16:03:10
Atomic Wallet.lnk	5/31/2020 16:03:10
atomicwallet.exe	5/31/2020 16:03:10
Bachelor Party de bone.xlsx	5/31/2020 16:03:10
be the match email.docx	5/31/2020 16:03:10
be the match.docx	5/31/2020 16:03:10
bethematch notes.docx	5/31/2020 16:03:10
Bill Phyxius Note.pdf	5/31/2020 16:03:10
BitTorrent Web.lnk	5/31/2020 16:03:10
Bones Bachelor Party Math.pdf	5/31/2020 16:03:10
Bones speech.docx	5/31/2020 16:03:10
brookyln kitchen.jpg	5/31/2020 16:03:10
btweb_installer.exe	5/31/2020 16:03:10
Call_History.xlsx	5/31/2020 16:03:10
Charleston CL.docx	5/31/2020 16:03:10

File Name	Timestamp Date/Time - UTC-05:00 (M/d/yyyy)[DST]
Cover Letter - Michael Knechtel.docx	5/31/2020 16:03:10
Cover letter northern Right.docx	5/31/2020 16:03:10
COW.jpg	5/31/2020 16:03:10
creepy_setup_v1.4.1_x86_64.exe	5/31/2020 16:03:10
dataconverter (1).7z	5/31/2020 16:03:10
dc ip.docx	5/31/2020 16:03:10
dread key.txt	5/31/2020 16:03:10
elementor.2.8.2.zip	5/31/2020 16:03:10
Example.xlsx	5/31/2020 16:03:10
Excel.lnk	5/31/2020 16:03:10
FULLLOCATION.xlsx	5/31/2020 16:03:10
gimp-2.10.12-setup-3.exe	5/31/2020 16:03:10
Git Bash.lnk	5/31/2020 16:03:10
Git-2.23.0-64-bit.exe	5/31/2020 16:03:10
grey medicus email pgp backup.txt	5/31/2020 16:03:10
grey medicus email pgp.txt	5/31/2020 16:03:10
h8mail-master.zip	5/31/2020 16:03:10
horseman note.txt	5/31/2020 16:03:10
icapital notes.docx	5/31/2020 16:03:10
IMG_1120 - Copy.MOV	5/31/2020 16:03:10
IMG_1120 - Copy.MOV.Mediainfo.txt	5/31/2020 16:03:10
IMG_1120 - Copy.MOV.VideoCleaner_settings.txt	5/31/2020 16:03:10
IMG_1120 - Copy.mp4	5/31/2020 16:03:10
IMG_1120 - Copy_2.mp4	5/31/2020 16:03:10
IMG_1120 - Copy_3.mp4	5/31/2020 16:03:10
IMG_1120.MOV	5/31/2020 16:03:10
IMG_1120.MOV.Mediainfo.txt	5/31/2020 16:03:10
IMG_1120.MOV.VideoCleaner_settings.txt	5/31/2020 16:03:10
IMG_1120xx2.ts.ffindex	5/31/2020 16:03:10
IMG_1120xx2.ts.Mediainfo.txt	5/31/2020 16:03:10
IMG_1120xx2.ts.VideoCleaner_settings.txt	5/31/2020 16:03:10
IMG_1702.JPG	5/31/2020 16:03:10
IMG_9965.JPG	5/31/2020 16:03:10
ip netflix 10.23.xlsx	5/31/2020 16:03:10
ip sig from netflix.xlsx	5/31/2020 16:03:10
ipscan-3.6.1-setup.exe	5/31/2020 16:03:10
ipscan-3.6.2-setup.exe	5/31/2020 16:03:10
ipscan-win64-3.6.1.exe	5/31/2020 16:03:10
jobs.docx	5/31/2020 16:03:10
John Letter.docx	5/31/2020 16:03:10

File Name	Timestamp Date/Time - UTC-05:00 (M/d/yyyy)[DST]
letter to self before point 72 interview.docx	5/31/2020 16:03:10
linkedin (2).jpg	5/31/2020 16:03:10
linkedin.jpg	5/31/2020 16:03:10
Maltego.lnk	5/31/2020 16:03:10
maltegotest.xlsx	5/31/2020 16:03:10
maltegotestip.xlsx	5/31/2020 16:03:10
Malwarebytes.lnk	5/31/2020 16:03:10
Mark Yusko - Final.mp3	5/31/2020 16:03:10
Mark Yusko second letter.docx	5/31/2020 16:03:10
MBSetup.exe	5/31/2020 16:03:10
Mere letter final.docx	5/31/2020 16:03:10
Mere Letter.docx	5/31/2020 16:03:10
Mere lettter final copy.docx	5/31/2020 16:03:10
meredith from the heart letter.docx	5/31/2020 16:03:10
meredith heart letter.docx	5/31/2020 16:03:10
metasploit-latest-windows-installer.exe	5/31/2020 16:03:10
Michael Knechtel EFT Form_encrypted_.pdf	5/31/2020 16:03:10
Michael Knechtel Resume Tech.docx	5/31/2020 16:03:10
Michael Knechtel Resume.docx	5/31/2020 16:03:10
Michael Knechtel Resume.pdf	5/31/2020 16:03:10
Michael Knechtel Resumetex.docx	5/31/2020 16:03:10
Milken Institute Cover Letter.docx	5/31/2020 16:03:10
Milken Institute Cover Letter.pdf	5/31/2020 16:03:10
MOBILedit Forensic.lnk	5/31/2020 16:03:10
muler pgp.txt	5/31/2020 16:03:10
nancy davis email.docx	5/31/2020 16:03:10
nancy davis quadratic email.docx	5/31/2020 16:03:10
nancy email 6.docx	5/31/2020 16:03:10
nancy letter 2.docx	5/31/2020 16:03:10
nancy letter 3.docx	5/31/2020 16:03:10
nancy letter 4.docx	5/31/2020 16:03:10
nancy letter 5.docx	5/31/2020 16:03:10
nancy marketing email 2.docx	5/31/2020 16:03:10
nancy marketing email.docx	5/31/2020 16:03:10
netflix ip 10.17.2019.xlsx	5/31/2020 16:03:10
netflix ips 2.docx	5/31/2020 16:03:10
NetflixViewingHistory.csv	5/31/2020 16:03:10
Nmap - Zenmap GUI.lnk	5/31/2020 16:03:10
nmap-7.80-setup.exe	5/31/2020 16:03:10
nping-0.7.80-1.x86_64.rpm	5/31/2020 16:03:10

File Name	Timestamp Date/Time - UTC-05:00 (M/d/yyyy)[DST]
number calls were forwarded to.txt	5/31/2020 16:03:10
orders(AutoRecovered).xlsx	5/31/2020 16:03:10
orders.xlsx	5/31/2020 16:03:10
orders2.xlsx	5/31/2020 16:03:10
Passware Kit Forensic Demo 2019 v4 (64-bit).lnk	5/31/2020 16:03:10
Patrol Sort (1).xlsx	5/31/2020 16:03:10
Patrol Sort (2).xlsx	5/31/2020 16:03:10
Patrol Sort.xlsx	5/31/2020 16:03:10
PDF+document.pdf	5/31/2020 16:03:10
pgp message from luscious.txt	5/31/2020 16:03:10
Phyxius Letter Bill.docx	5/31/2020 16:03:10
Phyxius Tear Sheet 2019.pdf	5/31/2020 16:03:10
Phyxius Tear Sheet Q1 2019 Final updated.pptx	5/31/2020 16:03:10
Phyxius Valuation (2).jpg	5/31/2020 16:03:10
Phyxius Valuation.jpg	5/31/2020 16:03:10
pic1 (2).jpg	5/31/2020 16:03:10
pic1.jpg	5/31/2020 16:03:10
PLACESS2 - Copy.csv	5/31/2020 16:03:10
PLACESS2.csv	5/31/2020 16:03:10
Point 72 mentorship cover letter 2.docx	5/31/2020 16:03:10
Point 72 mentorship cover letter.docx	5/31/2020 16:03:10
print_beam.pdf	5/31/2020 16:03:10
QuantShare.lnk	5/31/2020 16:03:10
QuantShareInstaller.exe	5/31/2020 16:03:10
questions for point72.docx	5/31/2020 16:03:10
Reinhardt olsen response.docx	5/31/2020 16:03:10
review_quadraticllc_com_2019-12-08 01_59_15.pdf	5/31/2020 16:03:10
robin hood cover letter.docx	5/31/2020 16:03:10
SafariHistory.xlsx	5/31/2020 16:03:10
Screen Shot 2019-11-05 at 10.45.52 AM.png	5/31/2020 16:03:10
shirts.xlsx	5/31/2020 16:03:10
sizes.xlsx	5/31/2020 16:03:10
smoking gun.txt	5/31/2020 16:03:10
SpiderFoot-2.12-w32.zip	5/31/2020 16:03:10
spruce cover ltter final.docx	5/31/2020 16:03:10
spruce cover ltter.docx	5/31/2020 16:03:10
sr recovery.txt	5/31/2020 16:03:10
testgps.csv	5/31/2020 16:03:10
testgps2.csv	5/31/2020 16:03:10
TESTLOCATIONXXXXX.csv	5/31/2020 16:03:10

File Name	Timestamp Date/Time - UTC-05:00 (M/d/yyyy)[DST]
TIP JAR.docx	5/31/2020 16:03:10
TIP JAR2.docx	5/31/2020 16:03:10
TIP JAR3.docx	5/31/2020 16:03:10
unix password.txt	5/31/2020 16:03:10
upwork writeup.docx	5/31/2020 16:03:10
user - PLACES (v1.0).csv	5/31/2020 16:03:10
VideoCleaner.txt	5/31/2020 16:03:10
VLC media player.lnk	5/31/2020 16:03:10
voicemailautomator-master.zip	5/31/2020 16:03:10
Yusko Letter 2.docx	5/31/2020 16:03:10
~$ddress.docx	5/31/2020 16:03:10
~$chael Knechtel Resume.docx	5/31/2020 16:03:10
altun	5/31/2020 16:03:10
testbot.py	5/31/2020 16:03:10
testbotmac.py	5/31/2020 16:03:10
a_testing	5/31/2020 16:03:10
Boxwood Cover Letter - Michael Knechtel.docx	5/31/2020 16:03:10
Boxwood Cover Letter - Michael Knechtel.pdf	5/31/2020 16:03:10
Michael Knechtel Resume - Copy.docx	5/31/2020 16:03:10
Michael Knechtel Resume Cohen.docx	5/31/2020 16:03:10
BOXWOOD RESUME AND COVER LETTER	5/31/2020 16:03:10
CCTClearcutLogger	5/31/2020 16:03:10
cleanup	5/31/2020 16:03:10
10.jpg	5/31/2020 16:03:10
1001016035_0_6y7b7j_l (1).jpeg	5/31/2020 16:03:10
09-30-2017 13_55_33.jpg	5/31/2020 16:03:10
1001016035_0_6y7b7j_l.jpeg	5/31/2020 16:03:10
back edit.jpg	5/31/2020 16:03:10
blender.lnk	5/31/2020 16:03:10
Call with bill.docx	5/31/2020 16:03:10
car.jpeg	5/31/2020 16:03:10
car.jpg	5/31/2020 16:03:10
check.jpg src=	5/31/2020 16:03:10
filmora-win_setup_full2065.exe	5/31/2020 16:03:10
final mere letter 2.docx	5/31/2020 16:03:10
final mere letter.docx	5/31/2020 16:03:10
FonePaw Video Converter Ultimate.lnk	5/31/2020 16:03:10
garage (2).jpeg	5/31/2020 16:03:10
garage.jpeg	5/31/2020 16:03:10
GitHub Desktop.lnk	5/31/2020 16:03:10

File Name	Timestamp Date/Time - UTC-05:00 (M/d/yyyy)[DST]
cleanup x	5/31/2020 16:03:10
cleanup2	5/31/2020 16:03:10
$RUNDJLW	5/31/2020 16:03:10
email address.txt	5/31/2020 16:03:10
$I7YVJVO	5/31/2020 16:03:16
Stellar Photo Recovery Professional 10.0.0.0 + Crack.zip	5/31/2020 16:03:16
$R7YVJVO	5/31/2020 16:03:16
$IUVYH88	5/31/2020 16:03:21
$RUVYH88	5/31/2020 16:03:21
IMG_0230.lnk	5/31/2020 16:04:22
Downloads.lnk	5/31/2020 16:04:23
IMG_0239.lnk	5/31/2020 16:04:27
026_Books.lnk	5/31/2020 16:04:38
20 MW (2).lnk	5/31/2020 16:04:38
chrome_shutdown_ms.txt	5/31/2020 16:04:43
$RZSXOTQ.bat	5/31/2020 16:19:56
$IZSXOTQ.bat	5/31/2020 16:19:56
$RUHBH6R.txt	5/31/2020 16:20:02
$IUHBH6R.txt	5/31/2020 16:20:02
$R79WLCY.txt	5/31/2020 16:20:07
$I79WLCY.txt	5/31/2020 16:20:07
vpn.cef	5/31/2020 16:24:38
glasswire - Copy.lnk	5/31/2020 16:25:54
$REMSE5K.pdf	5/31/2020 16:27:41
$IEMSE5K.pdf	5/31/2020 16:27:41
MANIFEST-000504	5/31/2020 16:28:21

23. Some of the items in the above table have names that start with a $R or $I. These are files that appear in the Recycle Bin when a user deletes a file. The original file is renamed to the $R name and its parent folder is modified to be the Recycle Bin. Its contents remain that of file that was deleted. The $I file contains information about where the $R file originally existed, its size, and when it was moved to the Recycle Bin. This allows the user to restore the file from the Recycle Bin if it chooses.

24. That these files were deleted from the Recycle Bin means that a user emptied the Recycle Bin manually or by using an application. A user can delete a file and bypass the Recycle Bin by pressing SHIFT-Delete. This is suggestive of a deliberate attempt to permanently delete data.

Forensics, Data Recovery, and Encryption Software

25. The following table shows folders that existed on a removable drive with Volume Serial Number 36E66023:

Linked Path	Target File Created Date/Time - UTC-05:00 (M/d/yyyy)[DST]	Target File Last Modified Date/Time - UTC-05:00 (M/d/yyyy)[DST]
G:\SysTools SSD Data Recovery 4.0.0.0 Final + Crack	3/17/2020 2:14	3/1/2020 16:49
G:\SysTools SSD Data Recovery 4.0.0.0 Final + Crack	3/17/2020 2:14	3/1/2020 16:49
G:\gpg4usb	3/17/2020 2:14	3/1/2020 17:17
G:\gpg4usb	3/17/2020 2:14	3/1/2020 17:17
G:\gpg4usb	3/17/2020 2:14	3/1/2020 17:17

26. GPG4USB[3] is a free, portable tool used for encrypting and decrypting messages and files. GNU Privacy Guard ("GPG") is a similar and compatible computer program to Pretty Good Privacy ("PGP"); both are used to protect electronic communication[4]. The above table shows that a folder with a name like the utility existed on a USB flash derive that was connected to the Laptop. According to the USN Journal, files with names indicative of being PGP encrypted messages or keys, such as "Pgp message from luscious.txt," "grey medicus email php.txt," and "grey medicus email pgp backup.txt" were created on the Laptop on March 24,

[3] https://www.gpg4usb.org/

[4] http://www.differencebetween.net/technology/software-technology/difference-between-pgp-and-gpg/

2020 and deleted on May 31, 2020. This is common when communicating with someone securely using PGP encryption.

27. SysTools SSD Data Recovery 4.0.0.0 Final + Crack is a program that recovers data from Solid State Hard Drives, which the Laptop does operate on. This file or folder was created on the removable drive (with Volume Serial Number: 36E66023) on March 17, 2020.

28. **MOBILedit Forensic Express**[5] is a forensic tool used for extracting data from mobile devices and generating reports about that data. A series of HTML reports were opened from a USB drive with (Volume Serial Number: 778AA449):

Linked Path	Target File Created Date/Time - UTC-05:00 (M/d/yyyy)[DST]
F:\199_Filesystems.html	3/20/2020 17:24:06
F:\005_Contact_Accounts.html	3/20/2020 17:23:57
F:\026_Books.html	3/20/2020 17:23:53
F:\004_Deleted_Data.html	3/20/2020 17:23:52
F:\003_Summary.html	3/20/2020 17:23:51
F:\196_Audio_Files.html	3/20/2020 17:23:50
F:\009_Calls.html	3/20/2020 17:23:49
F:\009_C7	3/20/2020 17:23:49
F:\010_Organizer.html	3/20/2020 17:23:42

29. Based on my review of the LNK files, the reports were generated on March 20, 2020 at approximately 11:52am, copied to the USB flash drive on March 20, 2020 at approximately 5:23pm, and opened and viewed on the Laptop on March 25, 2020. Chrome corroborated the association with the MOBILedit application, reporting the title for each HTML report being: “Apple iPhone X - fulliphone - MOBILedit Forensic Express.” The program and reports generated were deleted on May 31, 2020. This is suggestive that a user was viewing a report that was generated by mobile forensics software from an iPhone device.

[5] https://www.mobiledit.com/forensic-express/details

Generation of a Bootable USB Tool

30. Several artifacts indicate that attempts were made to create a bootable environment that can be launched from a USB device; there is also evidence that a bootable environment was downloaded. A bootable USB environment can be used to copy, modify, or delete data without leaving execution artifacts on the target system. Additionally, it can be used to repair software or hardware. The findings below indicate that the user had access to the tools needed to launch a bootable USB environment. The nature of such tools is that their use may not be detected in many instances; this is also why a user may choose to use them on a functional device such as a Laptop.

31. Between March 16, 2020 and March 17, 2020, internet history under the "Steven Brooks" user account on the Laptop recorded searches I infer to be related to the creation of a bootable USB drive, including: "create usb boot drive," "windows 10 iso download," "usb recovery windows 10 iso," and "windows 10 bootable usb tool."

32. The same day the user visited https://www.minitool.com/backup-tips/create-bootable-usb-from-iso.html, which presently displays an article detailing methods for generating a bootable USB device, and backing up and reinstalling Windows 10.

33. During this time, the Microsoft tool for creating a bootable Windows 10 recovery USB, "MediaCreationTool1909.exe", was also downloaded four times. Windows 10 disc images, "windowstan_Win10_1909_EnglishInternational_x64.iso" and "windowstan_Win10_1909_EnglishInternational_x32.iso" were also downloaded on March 17, 2020.

34. I identified a folder called "isolinux" on a removable drive that was connected to the Laptop, suggesting a bootable Linux environment was generated.

35. Internet history also shows a search for “rufus.” Rufus[6] is a utility used to create bootable USB drives, and it was referenced in the article mentioned in an earlier paragraph. The Rufus website, “https://rufus.ie/” was also accessed and the file “rufus-3.9.exe was subsequently downloaded on March 17, 2020 (Chrome history). A MUICache registry artifact indicates the Rufus executable ran sometime prior to March 24, 2020.

36. Internet history shows a search was conducted for “linux mint” on March 17, 2020. Linux Mint[7] is a version of another operating system, Linux, which can be installed to a computer or run from a USB drive in a bootable environment.

Cryptocurrency Software

37. An executable file “atomicwallet.exe” and a text file “atomic bitcoin wallet backup.txt” were identified. Atomic Wallet[8] is a secure cryptocurrency wallet for Bitcoin, Ethereum, Ripple, Litecoin, Stellar and various other coins. According to the USN Journal, the files were created on March 24, 2020 and deleted on May 31, 2020.

Alternative Accounts and Devices

38. Chrome stores data that a user had previously inputted into a website. The following table lists other email addresses that were identified through Chrome Auto Fill artifacts on the Laptop:

Email Address
morningsizz@protonmail.com
stevebrooks17@gmail.com
steven.brooks@libra.com
steven.brooks@libraarchive.com
steve.brooks@lxmgroup.com
sjb209@lehigh.edu
sbrooks14@gsb.columbia.edu

[6] https://rufus.ie/
[7] https://linuxmint.com/
[8] https://atomicwallet.io/

Email Address
shiptrader17 (Yahoo account)

39. On March 23, 2020, the user logged on to a Protonmail account with the user ID morningsizz@protonmail.com. Protonmail[9] advertises to be an end-to-end encrypted email service that allows users to send messages that will automatically be destroyed after a set amount of time for both the sender and the receiver.

New Device Notifications

40. Brooks may have transitioned to a new device in January 2020. This inference is based on the following:

a. 1/30/2020: The Steven.Brooks@libra.com account received an email from Justworks.com RE "New device login."

b. 2/03/2020 and 2/04/2020: The Steven.Brooks@libra.com account received emails with the subject "Security alert for your linked Google Account", which were moved the Deleted Items folder. The emails are related to the stevebrooks17@gmail.com account, of which steven.brooks@libra.com was the recovery account for.

c. 2/06/2020: The Steven.Brooks@libra.com account received an email regarding "We noticed a new sign into your Dropbox" which was located in the Deleted Items folder.

Security, Penetration Testing, and Hacking Software

41. The suite of software described below that was deleted from the Laptop is consistent with what would be on a device of an information security expert. However, it is

[9] https://protonmail.com/

inconsistent to have such software as a finance professional with no intent to delete or otherwise hide data.

42. The USN Journal indicates that the shortcut file for Passware Kit Forensic Demo 2019 (64-bit).lnk ("**Passware Kit**") was also created on the Laptop on March 24, 2020 and deleted on May 31, 2020. Passware Kit is a complete encrypted electronic evidence discovery solution that reports and decrypts all password-protected items on a computer. This program can be used to scan a computer for encrypted files and containers, extract encryption keys and passwords from a memory image, decrypt files, recover passwords on the device (including mobile and cloud), extract passwords for standalone system from external registry files, and create a USB or CD that resets Windows administrator password.[10] The existence of Passware Kit in combination with the failed attempts to access the Laptop's administrator account reinforces the possibility that the user was utilizing the software to obtain unauthorized control of the Laptop.

43. According to the USN Journal, the file named "metasploit-latest-windows-installer.exe" was created on the Laptop on March 24, 2020 and deleted on May 31, 2020. The Metasploit Project[11] is a computer security project that provides information about security vulnerabilities and aids in penetration testing and IDS signature development. Its best-known tool is for developing and executing exploit code against a remote target machine.

44. According to the USN Journal, files named "Maltego.lnk", "maltegotest.xlsx", and "maltegotestip.xlsx" were created on the Laptop on March 24, 2020 and deleted on May 31, 2020. Maltego is software used for open-source intelligence and forensics.[12]

[10] https://www.passware.com/kit-forensic/
[11] https://en.wikipedia.org/wiki/Metasploit_Project
[12] https://en.wikipedia.org/wiki/Maltego

45. According to the USN Journal, the file named "SpiderFoot-2.12-w32.zip" was created on the Laptop on March 24, 2020 and deleted on May 31, 2020. SpiderFoot is a reconnaissance tool that automatically queries over 100 public data sources to gather intelligence on IP addresses, domain names, e-mail addresses, names and more.[13]

46. According to the USN Journal, a file named creepy_setup_v1.4.1_x86_64" was created on the Laptop on March 24, 2020 and deleted on May 31, 2020. Creepy[14] is an open source intelligence tool used for gathering geolocation data from online sources and placing it on a map.

47. According to the USN Journal, the files named "Nmap – Zenmap GUI.lnk" and "nmap-7.80-setup.exe" were created on the Laptop on on March 24, 2020 and deleted on May 31, 2020. Nmap/Zenmap is a scanner used to identify devices on a network and perform queries such as displaying the open ports on a host or all hosts on a network.

48. According to the USN Journal, the files named "ipscan-3.6.1-setup.exe", "ipscan-3.6.2-setup.exe", and "ipscan-win64-3.6.1.exe" were created on the Laptop on March 24, 2020 and deleted on May 31, 2020. Angry IP Scanner[15] is a network scanner used to identify hosts and open ports.

49. According to the USN Journal, the file named "h8mail-master.zip" was created on the Laptop on March 24, 2020 and deleted on May 31, 2020. H8mail is a script that allows you find passwords or accounts that have previously been breached or to search local data. One can use this to check on themselves to identify if their login was leaked online post breach or to check on someone else's email/password combo).[16]

[13] https://www.spiderfoot.net/documentation/
[14] https://github.com/ilektrojohn/creepy
[15] https://angryip.org/
[16] https://github.com/khast3x/h8mail

50. Voicemailautomator is a proof of concept tool for research related to compromising account through cracking voicemail systems[17], (i.e. a hacking voicemail technique which allows you to compromise online accounts including PayPal, WhatsApp, Signal, Netflix, LinkedIn and others.[18] According to the USN Journal, the file named "voicemailautomator-master.zip" was created on the Laptop on March 24, 2020 and deleted on May 31, 2020.

Data Stored on Microsoft OneDrive and Other Cloud Platforms

51. Internet History on the Laptop identified the access of several cloud-based file storage services, including: OneDrive (shortcuts to online files remained through 6/19/2020) Box.com (accessed 1/28/2020), Dropbox (accessed 1/28/2020), Sky Drive (accessed 11/18/19), Google Drive (accessed on 2/27/2018).

52. Based on a review of the state of the Laptop at various restore points, the OneDrive account, associated with stevebrooks17@gmail.com, was first synchronized to the Laptop between 2/28/2020 and 3/17/2020.

53. I have identified at least 1,148 files stored in the OneDrive account, and many of the file and directory names appear to be related to Libra. These files are inaccessible from the Laptop unless the Laptop is online and signed into the associated Microsoft account. I confirmed that this is the case for all the files identified under the OneDrive folder hierarchy on the Laptop.

Failed attempts to login as administrator

54. The "Steven Brooks" user account was not in the administrator group, and so there may have been certain functions that user could not be performed using that account (e.g. installation of applications, accessing of system files, etc), depending on the security permissions

[17] https://github.com/martinvigo/voicemailautomator

[18] https://www.youtube.com/watch?v=E4UPlB2l8t8

of user accounts. Windows event logs indicated an abnormal number of failed logins during March 2020. This activity is consistent with the Passware program and suggestive of the user's attempt to access the administrator account on the Laptop.

55. Of the failed logins, March 2020 was the only time during this period which contained failed logins to the "Admin" user account, an account which is part of the administrator group. No successful logins to the "Admin" account were identified during this time.

Activity on dates where no activity was expected

56. SLG asked me to identify whether there was any activity on the following dates:

a. 2/28/2020 – There is activity on this date, including but not limited to, interactive logon to the Steven Brooks user account, USB storage device connected to Laptop, execution of user applications.

b. 3/20/2020 – There is activity on this date, including but not limited to, interactive logon to the Steven Brooks user account, web activity, and the deletion of files.

Other Custodian Devices

57. Regarding the preservation of other custodian devices, I was informed on June 26, 2020 by Andreas Mueller (on behalf of certain defendants) that he had generated forensic images for hard drives of Brian Mikkelson and Ted Hansen. Prior to this date, the preservation protocol of these systems had not been mutually agreed to.

I declare under the penalty of perjury that the foregoing is true and correct to the best of my knowledge and belief.

Dated: August 25, 2020

/s/ Aaron S. Weiss
Aaron S. Weiss